Network Incident Report

United States Secret Service/Financial Crimes Division/Electronic Crimes Branch

Telephone: (202) 406-5850 FAX: (202) 406-9233 E-mail: ecb@secretservice.gov

Status:

- ☐ Site under attack
- ☐ Incident investigation in progress
- ☐ Incident closed

What assistance do you require:

- ☐ Immediate call
- ☐ None needed at this time
- ☐ Follow-up on all affected sites
- ☐ Contact the "hacking" site(s)

Site involved (name & acronym):

POC for incident:

Name/Title _____

Organization _____

24 hr. x 7 d. contact information _____ E-mail _____

Alternate POC for incident:

Name/Title _____

Organization _____

24 hr. x 7 d. contact information _____ E-mail _____

Type of incident:

- ☐ Malicious code (i.e. virus, Trojan horse, worm...etc.)
- ☐ Probes/scans (non-malicious data gathering--recurring, massive, unusual...etc.)
- ☐ Attack (successful/unsuccessful intrusions including scanning with attack packets)
- ☐ Denial-of-service event
- ☐ High embarrassment factor
- ☐ Deemed significant by site

Date and time of the incident (specify time zone):

Summary of incident:

Type of service, information, or project compromised (please provide specifics):

- ☐ Sensitive unclassified such as privacy, proprietary, or source selection _____
- ☐ Other unclassified _____

Damage done:

Number of systems affected _____

Nature of loss, if any _____

System downtime _____

Cost of incident _____

Name of other sites contacted:

Law Enforcement _____

Other(s) _____

Details for Malicious Code

Apparent Source:

- ☐ Diskette, CD...etc.
- ☐ E-mail attachment
- ☐ Software download

Primary system or network involved:

IP addresses or sub-net addresses _____

OS version(s) _____

NOS version(s) _____

Other _____

Other affected systems or networks (IPs and OSs):

Type of malicious code:

Virus _____

Trojan/horse _____

Worm _____

Other _____

Copy sent to:

Method of Operation (for new malicious code):	**Details:**
☐ Type: macro, boot, memory resident, polymorphic, self encrypting, stealth	
☐ Payload	
☐ Software infected	
☐ Files erased, modified, deleted, encrypted (any special significance to these files)	
☐ Self propagating via e-mail	
☐ Detectable changes	
☐ Other features	

How was it detected:

Remediation (what was done to return the system(s) to trusted operation):	**Details:**
☐ Anti-virus product gotten, updated, or installed for automatic operation	
☐ New policy on attachments	
☐ Firewall, routers, or e-mail servers updated to detect and scan attachments	
☐ Other _____	

Additional comments:

Details for Probes and Scans

Apparent Source:

IP address _____

Host name _____

Location of attacking host: ☐ Domestic ☐ Foreign ☐ Insider

Primary system(s) or network(s) involved:

IP addresses or sub-net addresses _____

OS version(s) _____

NOS version(s) _____

Other _____

Other affected systems or networks (IPs and OSs):

Method of Operation:	**Details:**
☐ Ports probed/scanned ☐ Order of ports or IP addresses scanned ☐ Probing tool ☐ Anything that makes this probe unique	
How was it detected:	**Details:**
☐ Another site ☐ Incident response team ☐ Log files ☐ Packet sniffer ☐ Intrusion detection system ☐ Anomalous behavior ☐ User	

Log file excerpts:

Additional comments:

Details for Unauthorized Access

Apparent Source:

IP address _____

Host name _____

Location of attacking host: ☐ Domestic ☐ Foreign ☐ Insider

Primary system(s) or network(s) involved:

IP addresses or sub-net addresses _____

OS version(s) _____

NOS version(s) _____

Other _____

Other affected systems or networks (IPs and OSs):

Avenue of attack:	**Details:**
☐ Sniffed/guessed/cracked password ☐ Trusted host access ☐ Vulnerability exploited ☐ Hacker tool used ☐ Utility or port targeted ☐ Social engineering	

Level of access gained-root/administrator, user:

Method of operation of the attack (more detailed description of what was done):	**Details:**
☐ Port(s) or protocol(s) attacked ☐ Attack tool(s) used, if known ☐ Installed hacker tools such as rootkit, sniffers, 10phtcrack, zap...etc. ☐ Site(s) hacker used to download tools ☐ Where hacker tools were installed ☐ Established a service such as IRC ☐ Looked around at who is logged on ☐ Trojanned, listed, examined, deleted, modified, created, or copied files ☐ Left a backdoor ☐ Names of accounts created and passwords used ☐ Left unusual or unauthorized processes running ☐ Launched attacks on other systems or sites ☐ Other	

Details for Unauthorized Access (continued)

How detected::

- ☐ Another site
- ☐ Incident response team
- ☐ Log files
- ☐ Packet sniffer
- ☐ Intrusion detection software
- ☐ Anomalous behavior
- ☐ User
- ☐ Alarm tripped
- ☐ TCP Wrappers
- ☐ TRIPWIRED
- ☐ Other

Log file excerpts:

Remediation (What was done to return the system(s) to trusted operation):

- ☐ Patches applied
- ☐ Scanners run
- ☐ Security software installed
- ☐ Unneeded services and applications removed
- ☐ OS reloaded
- ☐ Restored from backup
- ☐ Application moved to another system
- ☐ Memory or disk space increased
- ☐ Moved behind a filtering router or firewall
- ☐ Hidden files detected and removed
- ☐ Trojan software detected and removed
- ☐ Left unchanged to monitor hacker
- ☐ Other

Details:

Additional comments:

Details for Denial-of-Service Incident

Apparent Source:

IP address _____

Location of attacking host: ☐ Domestic ☐ Foreign ☐ Insider

Primary system(s) or network(s) involved:

IP addresses or sub-net addresses _____

OS version(s) _____

NOS version(s) _____

Other _____

Other affected systems or networks (IPs and OSs):

Method of Operation:	**Details:**
☐ Tool used ☐ Packet flood ☐ Malicious packet ☐ IP Spoofing ☐ Ports attacked ☐ Anything that makes this event unique	
Remediation (what was done to protect the system(s)):	**Details:**
☐ Application moved to another system ☐ Memory or disk space increased ☐ Shadow server installed ☐ Moved behind a filtering router or firewall ☐ Other	

Log file excerpts:

Additional comments: